

• THE AGENCY PLAYBOOK

The Complete WordPress Security Guide

From zero to hack-proof WordPress sites.

THIS GUIDE IS DEVELOPED WITH



4

CHAPTERS

24

SECTIONS

What's inside

0.0 Learning to crawl Answering common security questions 03

Why would someone hack my site?

What are WordPress vulnerabilities?

What are the most common website hacks?

Why is getting hacked a big deal?

1.0 Learning to walk Understanding the basics 10

The three layers of WordPress security

Hosting providers

The human factor

How to choose a good host?

Host's vs. your responsibility

Why hosting security alone is not enough

2.0 Learning to run Hands-on knowledge and best practices 21

How to harden WordPress security

How to stay compliant with security?

What to do when your site gets hacked?

CRA compliance for WordPress agencies

The four-step incident response plan

CRA penalties

3.0 Learning to fly Automating proactive security at scale 33

Upgrading to proactive end-to-end security

How WP Umbrella secures your portfolio

What is virtual patching?

Layer 1: Security Base

Traditional plugins vs. virtual patching

Layer 2: The Security Add-on

The ideal WordPress security solution

WP Umbrella vs. traditional plugins

WHO THIS IS FOR

WordPress agencies, freelancers and care-plan providers who maintain more than one site.

WHAT YOU'LL WALK AWAY WITH

- 01 A working knowledge base of how WordPress security actually breaks
- 02 A 20-point hardening checklist
- 03 A recovery plan for the day a site gets hacked
- 04 How to choose the right security solution
- 05 How to choose the right hosting provider

0.0

Learning to crawl

Answering the common security questions every agency hears from clients.

IN THIS CHAPTER

- 01 Why would someone hack my site?
- 02 What are WordPress vulnerabilities?
- 03 What are the most common website hacks?
- 04 Why is getting hacked a big deal?

Why would someone hack my site?

Before diving into WordPress security, let's answer a simple question: **"Why would someone hack my site? It's small. I don't sell anything. Why would anyone bother?"**

The truth is that hackers don't really hand-pick sites. Therefore, most attacks aren't about size, traffic, or whether you handle payments or not. Instead, it's about targeting vulnerabilities that are often hidden in WordPress plugins.

How do hackers do it?

They run automated scans across countless IP addresses. If a site happens to be running a plugin with an exposed weakness, it becomes a target. One unpatched vulnerability in a popular plugin can give attackers access to thousands of sites at once. And if your site is among them and lacks the proper security setup, it could get hacked.



FROM THE FIELD

The moment you register a domain and put it online, you become a target. This isn't theoretical — we've tested it. We registered a brand-new domain, installed a dummy WordPress site, connected it to Patchstack, and tracked how long it took before the first attack attempt.

17

minutes until the first attack attempt

Being online automatically means being targeted.

Oliver Sild • CEO at Patchstack

KEY POINT

Attacks aren't aimed at you — they're aimed at a plugin you happen to run. Size, traffic and payments have nothing to do with it.

What are the most common website hacks?

We often call every website attack a "hack." But not all hacks are the same. Let's clarify the most common ones so you know what to watch for.

Malware

"bad code"

Malware is harmful software that sneaks onto your website and can steal data, spread spam, or redirect visitors to other shady sites. If it slips in, visitors may see random pop-ups, spam, or unsafe content. As a consequence, Google blacklists malware-infected sites to protect users from system damage, data theft, and malicious software downloads, causing traffic to drop fast.

Hack

"breaking in"

A hack happens when someone finds a weak spot, such as an outdated plugin or a weak password, to break into your site. Once inside, they might lock you out and demand ransom (remember the WannaCry ransomware), or steal sensitive client and visitor data. Recovery can be costly and take time, all while your site remains down or dysfunctional.

Brute force attack

"password guessing"

A brute force attack is when hackers use bots to try thousands of password combinations until they get the right one to access your website. Weak or reused passwords make it easier for them to orchestrate a fast break-in. If a brute force attack happens on one of your sites, admin accounts can be hijacked, giving hackers full control.

DDoS attack

"traffic jam"

DDoS (Distributed Denial of Service) attack is when hackers flood your server with fake traffic so real visitors can't get through. Your site could go offline, sometimes for hours or days, causing loss of legitimate traffic and revenue for your client during downtime.

SQL injection

"database break-in"

SQL Injection happens when hackers trick your website into giving them direct access to its database. They do this by sneaking malicious commands into places like login forms or search bars. Sites with outdated plugins or poorly coded forms are the most vulnerable.

KEY POINT

For WordPress specifically, most attacks come from exploiting vulnerabilities in existing themes or plugins. Next, we'll cover what vulnerabilities really are.

What are WordPress vulnerabilities?

A vulnerability is a flaw in the code logic that exposes a weakness in software that can be exploited. In WordPress, they appear in core, themes, or plugins. They don't exist because the software is poorly made, but because even the best software can develop vulnerabilities over time as technology advances and sophisticated attack methods emerge. So even the most well-built plugins and themes can have weak spots waiting to be discovered.



We often hear about two types of vulnerabilities:

ZERO-DAY

Exploited before the plugin developers even know about the issue, often within hours of discovery.

ONE-DAY

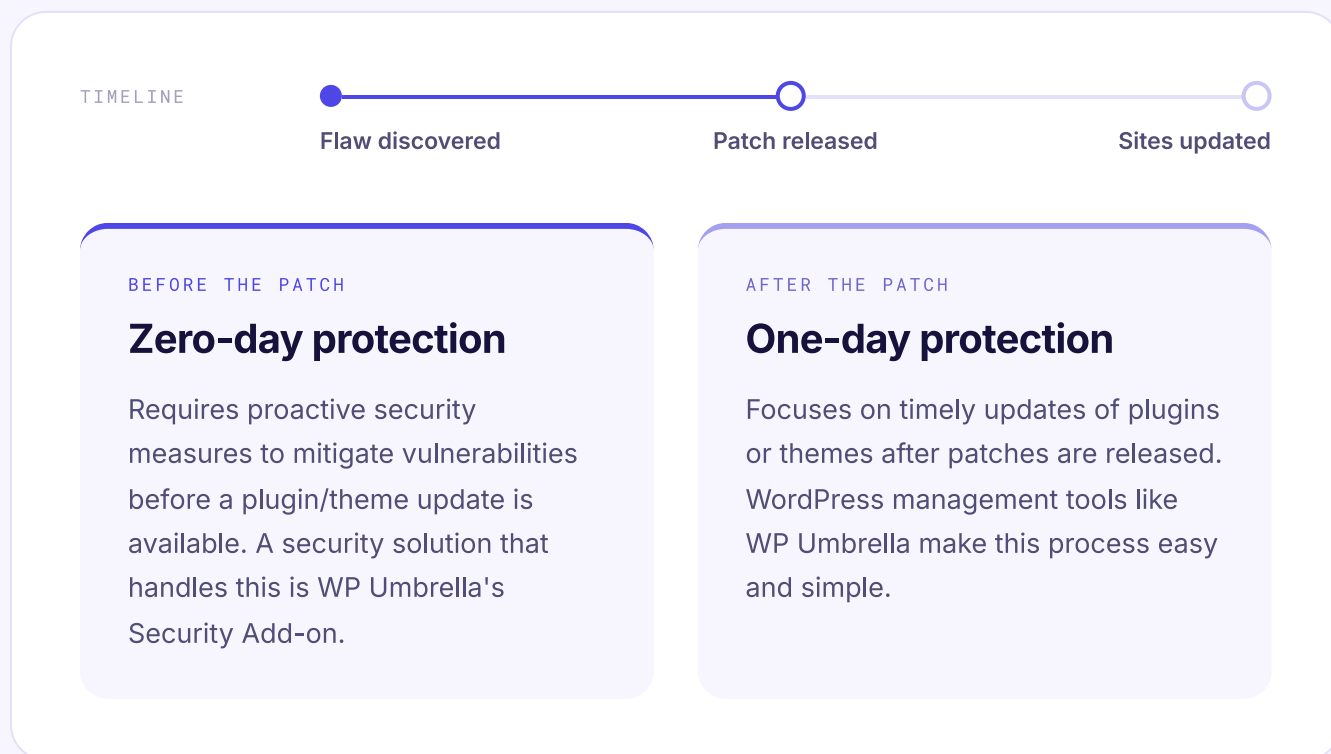
Exploited after the plugin developers release a vulnerability patch. Hackers watch plugin changelogs, then rush to attack sites that haven't updated the plugin yet.

To fix vulnerabilities, you need to keep plugins, themes, and WordPress core updated as often as possible. But updates alone won't secure your sites from everything. With over 80,000 plugins in the ecosystem, new flaws are found all the time, and attackers often strike before site owners or developers can patch them. The best way is to take proactive steps instead of reacting to an issue.

¹ Full details available at: patchstack.com/whitepaper/state-of-wordpress-security-in-2025/

How to protect against plugin vulnerabilities?

Each vulnerability type opens a different window of exposure — and each needs a different answer.



Why is getting hacked a big deal?

The impact of any of the website attacks we explained before isn't just technical — it can also be financial, reputational, and operational. But what exactly could go wrong?

01	SEO damage	A hacked site often gets blacklisted, dropping out of Google rankings. Even after cleanup, recovery can take weeks or months, costing traffic and revenue.
02	Ransomware	Attackers may lock the site and demand Bitcoin payments to restore it. Without proper backups, site owners are stuck in a very uncomfortable position.
03	Malware and data theft	Website visitors can be infected, and their payment data can be stolen. A scenario like that can cause major damage to a brand's reputation, from which some businesses may never recover.
04	Resource hijacking	Attackers might use a site to host spam, run redirects to other suspicious websites, or even join botnets.
05	Regulatory fines	If customer data is exposed during the hack, the site owner could face penalties under laws like GDPR and CCPA.

These are some scenarios that can follow if a site gets hacked. Cleaning up the mess is not easy, and even after it's fixed, trust and search rankings may take a long time to recover. But a proper security setup can prevent these problems, and we'll explain how later in this guide.

0.0 Learning to crawl

- 1 Hackers rarely target specific sites. Instead, they scan the web in bulk for vulnerable plugins or themes and attack any site with weaknesses.
- 2 Common attacks include malware, brute force, DDoS, SQL injections, and general hacks. But in the WordPress world, plugin vulnerabilities are by far the most common entry point.
- 3 A WordPress vulnerability is a weakness in software (plugin, theme, or WordPress core) that attackers can exploit.
- 4 Zero-day vulnerabilities are exploited before developers even know about them, while one-day vulnerabilities are exploited after a patch is released but before sites are updated.
- 5 Getting hacked can have serious consequences: it can damage SEO, steal data, hijack resources, trigger ransomware, and even result in regulatory fines.

1.0

Learning to walk

Understanding the basics of WordPress security — and who is responsible for what.

IN THIS CHAPTER

- 01 The three layers of WordPress security
- 03 The human factor
- 05 Hosting providers

- 02 How to choose a good host?
- 04 Host's vs. your responsibility
- 06 Why hosting security alone is not enough

The three layers of WordPress security

To help us visualise this better, the WordPress security experts at Patchstack compare website security to a layered cake² — with the network, server, and application layers stacked on top of each other. Each layer defends against different types of weaknesses, and no single tool can protect them all. Let's break down what each layer does and why it matters.

FIGURE 2 · THE SECURITY STACK

ATTACK IN ————— THREE LINES OF DEFENCE ————— YOUR SITE

01

Network

Filters incoming traffic to block bad actors before they reach your site.

Stops DDoS, bad bots, known-bad IPs

02

Server

Protects your website's files, databases, and server environment from intrusions.

Stops damage once the door is open

03

Application

Secures WordPress itself, including themes, plugins, and logins, against site-specific attacks.

Where most WordPress attacks land

+ THE HUMAN FACTOR

Wraps all three — the cherry on the cake, and the layer most often forgotten.

² Learn more here: patchstack.com/articles/cheese-cake-and-cybersecurity-protecting-your-wordpress-website/

01 The network layer

"the front door"

The network layer is the first point of contact for traffic. It's like the "front door" to your website, controlling who or what can get in.

At this layer, security focuses on filtering traffic and keeping the bad actors out before they even get a chance to touch the next two layers — your server or your WordPress site.

Some tools that are helpful in this context are firewalls. They block DDoS attacks, malicious bots, or traffic from IP addresses that are known to be bad. They're essential to network security, but at the same time quite limited as well. Since they filter broadly, some threats can still slip through, and additional measures are needed to protect the server and the application layer.

02 The server layer

"the inside of your house"

If the network layer is the front door, the server layer is "the inside of your house". It's where your website's files, databases, and server software live.

Security at this layer is about making it hard for an intruder to do any damage, even if they somehow get past the front door. Some ways in which this is done are: regular software and OS updates, server isolation, backups, file integrity checks, and malware scanning.

As a critical part of your site's security, server-level protection is typically handled by your hosting provider. That's why choosing a reliable host that prioritizes security is so important. Later, we'll dive into what responsibilities fall on you as an agency and what your host should handle when it comes to keeping your sites safe.

03 The application layer "the living space"

The application layer is the "living space" of your website inside the server house. It's everything your visitors interact with: your themes, plugins, posts, pages, and the WordPress core itself. Security at this layer is about protecting the site itself from attacks that could exploit weaknesses in the code or configuration.

Know that the application layer is where most WordPress-specific attacks happen. Even if your server and network layers are secure, a vulnerable plugin or weak login can still put your site at risk. That's why ongoing maintenance is essential for WordPress sites, with care plans designed to keep the application layer secure at all times.

The human factor

The human factor is the cherry on top of the three-layered WordPress security cake. You could do everything right and still get hacked if one of your teammates decides to make his password "cake123."

To minimize risks from human error, both your team and your clients can follow these common-sense practices:

Least privilege access

Only grant admin roles when necessary and avoid giving users more permissions than they need.

Activity logs

Monitor user actions to spot suspicious behavior early.

Strong, unique passwords

This one is a no-brainer.

Two-factor authentication (2FA)

Adds an extra layer of login protection.

reCAPTCHA

Helps reduce bot traffic on certain sites.

Move your login page

Changing the default `/wp-login` URL can also reduce attack risk.



Oliver Sild

CEO at Patchstack

Agencies should avoid giving customers administrator accounts whenever possible. One of the most common issues we see is admin access in the hands of users with poor cyber hygiene.

They may use weak passwords, reuse the same password across multiple services, or have credentials exposed in data breaches. On top of that, their devices can be compromised. Some browser extensions collect session cookies from WP Admin, and those cookies are actively sold on dark markets. In some cases, attackers can literally buy access to WordPress admin accounts.

So, simply avoiding unnecessary admin accounts already makes a huge difference. If you absolutely must give someone administrator access, then make sure they use a password manager.

Ultimately, it's important to keep educating your teams and clients about why these measures matter. Small steps for protection are often overlooked because we think they won't make a lot of difference. But a single weak password can sometimes undermine your entire security setup.

Hosting providers

Since hosting providers do most of the security heavy lifting at the server layer, it's important to understand what their responsibilities are (vs. yours) and how to choose a reliable hosting partner. Six areas decide how secure a hosted WordPress site really is.

TABLE 1 · SPLIT OF RESPONSIBILITY – 1 OF 2

AREA	HOST'S RESPONSIBILITY	YOUR RESPONSIBILITY
01 Secure Connections	A good host should give you a free SSL certificate, so your site runs on HTTPS. This means all data (such as login details or form entries) is safely “locked in an envelope” when traveling between your visitor's browser and your site. Without HTTPS, that data travels like a postcard anyone can read, making it easy for attackers to steal.	Enforce HTTPS across your site so no traffic slips through unencrypted.
02 Backups	Hosts usually provide automated backups, which allow you to restore your site quickly in case of a website attack.	Relying only on your host's backups is not the best strategy. It's like keeping an important document and its copy in the same file: if disaster strikes, both could be lost at once. That's why double-backups are essential. Let your host handle one, and maintain a separate offsite backup that you can access independently if your host is ever unavailable or in trouble. WP Umbrella is the ideal solution for keeping a reliable offsite backup that can be restored in one click at any time.
03 Firewalls	Your host should provide and maintain network firewalls (and ideally a web application firewall — WAF) to block malicious traffic before it reaches your site.	Add DNS-level protection, like Cloudflare, which filters traffic before it even reaches your server. Then add application-level protection on top, like WP Umbrella's Firewall & Virtual Patching, which blocks specific, disclosed WordPress vulnerabilities at the PHP level, something a generic host WAF isn't built to catch.

RULE OF THUMB

Never keep the document and its only copy in the same drawer — one backup with the host, one offsite. Once every 24h is a good baseline; more often for high-activity sites.

Scanning, isolation & updates

AREA	HOST'S RESPONSIBILITY	YOUR RESPONSIBILITY
04 Malware Scanning	Malware scanning at the host level is more reliable compared to malware scanning done through a traditional plugin. That's because these plugins only work at the application level. If a hacker breaks into your site, they could disable or tamper with the plugin to cover their tracks. But even then, proactivity is the key to real security. Instead of adopting "scan and 1-click cleanup" as the main strategy, hosts should aim to locate and fight the source of the malware so that it doesn't get there in the first place.	Pair host-level scanning with a scanner that also runs off the site, like WP Umbrella's Security add-on. It scans every connected site daily from its own infrastructure, not a plugin sitting on the site, so it can't be disabled or tampered with the way an on-site plugin can. It also checks deeper than known threats: core files, every plugin and theme (including ones outside the official store), uploads, scheduled tasks, and supply-chain changes.
05 Server Isolation	Hosts often separate websites on the same server using containerization or virtualization. This way, if one site gets hacked, it doesn't spread problems to others.	Only hosting providers can set up proper server isolation, but your responsibility is to choose a reliable host that takes this seriously. Or educate and guide your clients on how to make that decision on their own.
06 Updates	Keep the server's operating system and software patched so hackers can't exploit weaknesses at the server level.	Keep WordPress itself (core, plugins, themes) updated. Hosts don't touch these, and most attacks happen here.

WHAT THIS ADDS UP TO

A great host removes a large share of your risk at the network and server layers — but never the application layer. Everything WordPress-specific stays yours: the plugins, the themes, the logins, the updates, and the second backup.

How to choose a good host?

Your hosting provider gives you the space and technology to store and run your website on the internet. But it's also the foundation of your WordPress security and performance. That's why choosing the right partner would be vital for a smooth WordPress experience. Here are the seven features to insist on:



"A good host doesn't just keep your site online, but it keeps it safe too! If you're considering shared hosting, make sure your provider follows best practices with proper isolation between accounts. Environments using CloudLinux with CageFS are a solid sign that your site will be protected from noisy neighbors."

Boris Zarev • Head of Support at WP Umbrella

01

Robust Security

Ensure you know exactly what the host does for security. Don't fall for vague "we're secure" claims.

02

Automatic HTTPS

Free, auto-renewing SSL certificates should be included by default.

03

Server Isolation

Check that the host uses containerization or virtualization to isolate sites from one another.

04

Reliable Performance

Look for fast servers, high uptime, CDN support, and scalable resources for growth.

05

WordPress Expertise

Managed Hosting with WordPress expertise acts less like a landlord who just rents you space, and more like a property manager who knows the building inside and out.

06

Backup & Recovery

A good host should automatically back up your site and allow for simple site restoration when needed. Ask about the backup frequency. Once every 24h is a great rule of thumb, but for high-activity sites, more frequent backups are recommended.

07

Responsive Support

Access to knowledgeable WordPress customer service will be essential, especially if you host multiple sites with the same provider.

All seven — not five.

The one question to ask a hosting provider



FROM THE FIELD

“What relationships do you have with security companies and the wider community?” If they have none, they're missing critical information and may not be able to respond effectively to security threats.

Oliver Sild • CEO at Patchstack

Choosing a hosting provider that meets all these criteria might not be the most budget-friendly option. But when it comes to hosting, going for the cheapest choice will (in most cases) cost you more in security risks and performance impact.

If you want to learn more on how hosting decisions impact speed, security, and profit, check out WP Minute's free course “Hosting Decoded: How to Choose the Best Host for WordPress” taught by Eric Karkovack.³

KEY POINT

A host with no ties to the security community is flying blind. Cheap hosting is not cheap once you price in the incidents it fails to stop.

³ Hosting Decoded: How to Choose the Best Host for WordPress – thewpminute.com/course/hosting-decoded-how-to-choose-the-best-host-for-wordpress/

But why is hosting security alone not enough?

What if you have all your sites with a host that has firewalls, anti-DDoS measures, and plenty of server-level protections? Is your site safe then? First of all, well done. You've made a great investment in your site's security. But there's still work to be done.

PATCHSTACK TESTED IT - TWICE

87.8%

of attacks bypassed hosting defenses entirely — across eleven common WordPress-specific vulnerabilities and five hosting providers.⁴

2025 study

~74%

of attacks still succeeded when the same experiment was repeated with a bigger statistical sample.⁵

2026 study

So why does this happen? Hosting security is designed to stop broad, generic threats, but not necessarily from plugin and vulnerability risks. These vulnerabilities are often invisible to standard server-level defenses because they don't match the patterns these systems are built to detect.

Therefore, hosting security alone isn't enough. To truly protect a WordPress site, you need an additional layer of defense at the application level. One that actively monitors for WordPress-specific vulnerabilities and blocks attacks in real time. Without it, even sites on “secure” hosting remain exposed and vulnerable. More on this in the next sections.

⁴ 2025 research: patchstack.com/articles/hosting-security-tested-87-percent-of-vulnerability-exploits-bypassed-hosting-defenses/

⁵ 2026 research: patchstack.com/articles/myth-of-secure-hosting-only-26-percent-of-vulnerability-exploits-blocked-by-hosts/

1.0 Learning to walk

- 1 There are three layers of WordPress security: network, server, and application layer. Each one defends against different types of weaknesses with different security measures.
- 2 The human factor can undermine even the most effective security strategies. Apply simple yet crucial practices, such as strong, unique passwords, 2FA, and least-privilege access.
- 3 Hosting providers do most of the security heavy lifting at the server layer. It's your responsibility to pick a reliable host for your sites.
- 4 Relying only on your host's backups is risky. If disaster strikes, both the original and the backup could be lost. Keep one copy with your host and a separate one offsite.
- 5 Hosting security alone isn't enough. To truly protect a WordPress site, you need an additional layer of defense at the application level.

2.0

Learning to run

Hands-on security knowledge, incident response, and staying compliant.

IN THIS CHAPTER

- 01 How to harden WordPress security
- 02 How to stay compliant with security?
- 03 What to do when your site gets hacked?
- 04 CRA compliance for WordPress agencies
- 05 The four-step incident response plan
- 06 CRA penalties

How to harden WordPress security

Now that we've looked at what can go wrong and what the different layers of security are, let's talk about what you can do to make your WordPress sites harder to break into. Here are some ways in which you can harden your WordPress security.

20 MEASURES · PART 1 OF 3

01

Use only reputable plugins

Poorly coded plugins are the most common source of WordPress vulnerabilities. Stick to well-known, actively maintained plugins with positive publicly available reviews from other users.

02

Update regularly

Keep WordPress core, plugins, and themes up to date. Updates help with known vulnerabilities.

03

Use proactive security solutions

WP Umbrella's Security Add-on monitors vulnerabilities in real time and applies virtual patches to protect your site before attacks occur.

04

Block access to directories

A directory listing shows the contents of folders when no index file exists. Disable directory browsing to hide files.

05

Rename the admin account

Instead of the default "admin" username, use a unique name to make brute-force attacks harder.

06

Use a custom database prefix

Changing the default `wp_` prefix slightly obscures your database tables. It's not a major defense, but it can help against automated attacks.

07

Disable PHP execution in certain folders

Uploaded files can be risky if PHP scripts run. Disable PHP execution in upload directories to prevent malicious code from running.

08

Follow the principle of least privilege

Give users only the permissions they need. Admin rights should be limited and temporary where possible. Audit user roles regularly and remove or downgrade unused accounts.

09

Limit login attempts

Protect your site from repeated password guessing by restricting the number of login attempts and using cooldown periods.

10

Password-protect sensitive paths

Some pages (like [phpinfo.php](#)) contain sensitive information. Add HTTP authentication to protect these paths.

11

Move wp-config.php to the parent directory

This critical file contains database credentials and security keys. Moving it outside the public web directory prevents attackers from accessing it directly.

12

Disable file editing in the dashboard

Prevent admins from editing plugin or theme PHP files through WordPress. This blocks hackers from injecting malicious code if they gain access.

13

Change the default SSH port

Using a non-standard port makes it harder for automated bots to attack your server.

14

Change the WordPress login URL

Hiding your login page from [/wp-login.php](#) reduces bot attacks that repeatedly try to guess passwords.

15

Block public SSH access

Only allow SSH connections from trusted IPs or use managed access solutions like a bastion host or cloud provider session managers.

16

Use SSH keys instead of passwords

SSH keys are far more secure than passwords and nearly impossible to brute-force.

17

Use strong passwords or passkeys

Simple passwords can be cracked in seconds. Use complex, unique passwords with uppercase, lowercase, numbers, and symbols. Enable two-factor authentication (2FA) for extra protection.

18

Block XMLRPC

XMLRPC lets WordPress run code remotely and transfer data. It's a feature that has become obsolete these days. Turn it off if you're not using it, as it can be exploited for brute-force attacks.

19

Avoid using the root account

Use a limited user account for SSH access. Root access is risky because it can make critical changes if compromised.

20

Configure HTTP headers⁶

HTTP headers are instructions sent by the server to the browser that can enhance website security. Configure Content Security Policy (CSP), X-XSS-Protection, Cross-Origin Resource Sharing (CORS), and Strict-Transport-Security (HSTS). This protects against attacks like XSS, data injection, and cross-site scripting.

QUICK TIP

Instead of thinking of passwords — think of **pass-phrases**. A pass-phrase is a full sentence, something you can still easily remember, but for computers it's much harder to brute-force. The longer length makes it significantly more secure than a traditional password.

⁶ More guidance available here: patchstack.com/articles/hardening-wordpress-a-checklist-to-get-started/

What to do when your WordPress site gets hacked?

No matter how careful you are, WordPress sites can still get hacked. When a breach happens, what makes a big difference is if you have these 3 things:

01

Recent backups you can easily restore

02

A monitoring system that alerts you quickly

03

A clear incident response plan defining who does what

FIGURE 3

WordPress hack response plan

STEP 0

Before a Breach

Setup backups, monitoring, and have a clear incident plan.

STEP 1

Spot the Problem

Identify red flags, confirm the breach, and figure out which parts of your site are affected.

STEP 2

Contain the Damage

Take site offline, change passwords, revoke access, and disable affected plugins or themes.

STEP 3

Cleanup and Recover

Restore from backups. Update systems and activate a proactive security solution. Finally, get your site back online.

STEP 4

Learn from the Incident

Document breach and refine response plan as you go.

Step 1 Spot the problem

If a security problem occurs, the sooner you identify that your site is compromised, the less damage it can cause. Red flags to watch for are: shady redirects, spammy ads, unfamiliar admin accounts, strange new content, or even a sudden performance slowdown or a crash. But you can't watch every site all the time, so having automated alerts from a reliable monitoring system is crucial. Once you spot an anomaly:

- ☐ Confirm it with server logs and security tools.
- ☐ Check if you have any warnings in your Google Search Console's "Security Issues" under the "Security & Manual Actions" section.
- ☐ Get in touch with the hosting provider to check whether the other websites on the same server are showing similar signs.
- ☐ Then, figure out which parts of your site are affected: plugins, themes, core files, or the database. Understanding the scope is key to a clean recovery.

Step 2 Contain the damage

Breach confirmed? Now it's time to act fast.

- ☐ Take the site offline temporarily or enable maintenance mode to prevent attackers from doing more damage.
- ☐ Change all passwords — hosting, FTP, database, WordPress admin, and any linked email accounts.
- ☐ Review all user accounts and roles in WordPress and your hosting panel. Remove suspicious accounts and make sure only trusted users keep admin privileges.
- ☐ Given that you've already identified which parts of your site are affected, disable relevant plugins or themes until they're patched.
- ☐ Even if your site is hacked, make a backup of its current state before cleaning up. Keep it separate from your safe pre-hack backups. If something goes wrong during cleanup, you'll have a recovery point.
- ☐ And if your site is part of a network, make sure to isolate other sites in order to stop the infection from spreading.

Step 3 **Cleanup and recover**

This is where your clean, secure backups come to the rescue.

- ☐ Replace infected files with your safe copies and test everything carefully to make sure it works as expected: forms, shopping carts, and custom code.
- ☐ Then go ahead and update WordPress core, plugins, and themes to their latest versions.
- ☐ And since real recovery is about making your site stronger and safer than before, activate a proactive security solution that will prevent future vulnerability exploits.
- ☐ Finally, after the threat is removed, it's time to get your site back online.

Step 4 **Learn from the experience**

Going through a hack is terrible, but it's also a chance to find your blind spots and improve your defenses.

- ☐ Document what happened, the timeline, what was exploited, and what you did to fix it. For serious breaches, a forensic analysis by a security expert can reveal the root cause.
- ☐ Run a full antivirus scan on your PC or laptop to make sure that whatever infected your website doesn't impact your computer as well.
- ☐ And finally, communicate calmly with your client, or users, if any sensitive data was exposed. Transparency builds trust and strengthens the relationship.

FROM THE FIELD



Even when applying all WordPress security best practices, security is never something you achieve once and for all. It's an ongoing process that requires vigilance, updates, and sometimes an external audit to stay one step ahead of threats.

Thomas Deneulin • CTO at WP Umbrella

A breach doesn't have to be catastrophic. With preparation, fast detection, and a structured response, you can minimize downtime, protect your client and users, and keep your WordPress site secure. To ensure your incident response plan works when you need it, run regular simulation drills and continuously refine it based on best practices and real-world learnings.

PRACTISE IT

Drills

A response plan nobody has rehearsed is a document, not a plan.
Schedule a simulation once per quarter and note what slowed you down.

How to stay compliant with security?

Securing your WordPress site protects your users, your clients, and your business. But there's another reason why it matters so much. That's compliance with laws like the EU's Cyber Resilience Act (CRA).

The EU's Cyber Resilience Act introduces mandatory cybersecurity requirements for all digital products sold or distributed in the EU, including hardware and most software. It aims to fix two main gaps:

GAP 1

Lack of built-in security and reliable updates across digital products.

GAP 2

Lack of transparency about vulnerabilities and fixes.

To address these issues, the law introduces two sets of requirements: security during development and product design, and a formal vulnerability handling process, including disclosure and patching.

MANDATORY BY

Dec 2027

If your product is used in the EU — regardless of where you are based — and has any commercial element, CRA compliance will be mandatory.

CRA compliance for WordPress agencies

Most agencies act as distributors or importers when they deploy third-party software. That includes installing plugins from WordPress.org or bundling themes with new builds. In those roles, you're expected to verify that the products you use meet CRA standards.

That doesn't mean auditing every line of code, but it does mean knowing where the Software Bill of Materials (SBOM) lives, understanding how security updates are handled, and keeping that documentation on file.

FOR CARE-PLAN PROVIDERS

The implications are even more immediate. CRA sets expectations for how fast security incidents must be handled. That means separating feature updates from security patches is a legal necessity. If a plugin you manage has a critical vulnerability, it may require action within hours instead of waiting for the next sprint.

This changes client communication too: care reports may need to include details on when patches were applied, along with risk assessments, update logs, and mitigation steps.

There's also a broader risk: many agencies build one-off solutions using free plugins and quick integrations that no longer meet CRA standards. If you're deploying a free plugin that hasn't been updated in years, doesn't disclose vulnerabilities, or lacks SBOMs, you're introducing legal risk to your client and to yourself.

Agencies need to start thinking in terms of traceability

Right now, that kind of information is scattered across spreadsheets, emails, and staging servers. Under CRA, that won't be enough. You have to be able to answer four questions for every site you manage:

Which software runs on which sites?

When was it last updated?

Is there documentation available if it breaks or gets breached?

Who owns the patching process?

Agencies that provide care plans or manage websites on behalf of clients will need to adapt their stack, their workflows, and their documentation habits. They will have to treat maintenance like a compliance service, not just a support retainer.

CRA penalties

The Cyber Resilience Act introduces serious enforcement mechanisms for non-compliance.

€15 million

or 2.5% of turnover

Whichever is higher, for failure to meet essential security requirements (e.g., secure-by-design, vulnerability handling).

€10 million

or 2% of turnover

For breaches of other obligations (documentation, incident reporting).

€5 million

or 1% of turnover

For supplying false or misleading information.

Importantly, member states have the authority to impose additional consequences, such as recalling a non-compliant product or ordering its withdrawal from the EU market.

2.0 Learning to run

- 1 Some of the most important steps you can take to harden WordPress security are running frequent updates and activating a proactive security solution like WP Umbrella's Security Add-on.
- 2 Just in case, prepare reliable backups stored offsite, real-time monitoring for quick alerts, and a clear incident response plan for any security crisis.
- 3 In a website attack, act fast: detect the issue, contain the damage, clean up, and recover. Then review the incident and refine your response plan for next time.
- 4 EU's Cyber Resilience Act mandates built-in security, transparent vulnerability handling, and proper documentation for all digital products in the EU. It covers serious penalties for non-compliance, and care plan providers can be affected.

3.0

Learning to fly

Automating proactive WordPress security at scale, across a whole portfolio.

IN THIS CHAPTER

- 01 Upgrading to proactive end-to-end security
- 02 How WP Umbrella secures your portfolio
- 03 What is virtual patching?
- 04 Layer 1: Security Base
- 05 Traditional plugins vs. virtual patching
- 06 Layer 2: The Security Add-on
- 07 The ideal WordPress security solution
- 08 WP Umbrella vs. traditional plugins

Upgrading to proactive end-to-end WordPress security

At its core, the CRA demands proactive protection. It wants digital elements “secured by design”. It expects measures that reduce the attack surface before vulnerabilities are exploited.

And that's what WordPress security should be all about. It should go beyond malware scans and cleanup services. And it should put systems in place that block known threats, enforce secure defaults, and create a traceable record of how vulnerabilities are handled.

THE PACE OF THE PROBLEM

All of 2022

1×



January 2026 alone

3×



VULNERABILITY REPORTS RECEIVED

In January 2026 alone, Patchstack received about three times as many vulnerability reports as the entire year of 2022. The speed at which threats appear is increasing, but the time agencies have to respond is shrinking.

AI has collapsed the time between a vulnerability going public and a working exploit existing in the wild. So, if security isn't automated in some way, WordPress agencies risk falling behind attackers who're automating their attacks extensively.

The only defense that still works at that speed is one that blocks the exploit attempt itself, before an update is even possible.

THAT DEFENSE IS

Virtual patching

What is virtual patching?

Virtual patching is the technology that stops hackers from taking advantage of security holes before they can do any damage. It acts like deploying a shield on demand in front of a vulnerable part of your website, without actually changing the website itself.

DEFINITION · OWASP

The Open Worldwide Application Security Project (OWASP) — a nonprofit foundation that works to improve the security of software — defines virtual patching as a **“security policy enforcement layer which prevents the exploitation of a known vulnerability.”**

When a vulnerability is found in a plugin, it's usually documented with a CVE (Common Vulnerabilities and Exposures) ID. Security researchers (or platforms like Patchstack) study the vulnerability and figure out exactly how an attacker could exploit it. That information then becomes the virtual patch.

PRECISE

A virtual patch watches all incoming traffic (HTTP requests) and blocks only the requests that try to exploit that specific bug.

FEWER FALSE POSITIVES

Unlike generic WAF filters that often rely on broader pattern detection, virtual patches are very precise.

ZERO-DAY READY

Effective even when a vulnerability is being exploited in the wild and no official fix exists yet.

It protects your site immediately without breaking functionality, giving you time to wait for the official fix of the vulnerability.

Traditional security plugins vs. virtual patching

REACTIVE

Traditional security plugins

Most WordPress security plugins look for problems after they've already happened. They check files or monitor behavior to find infections, but they don't stop attacks before they occur.

They can also miss cleverly hidden malware, slow down the server, and sometimes give false alarms, especially when scanning frequently.

PROACTIVE

Virtual patching

Virtual patching doesn't rely on file changes or behavioral analysis. Instead it blocks attacks before they reach the site by stopping known exploit patterns in real time.

Since it focuses on requests (using targeted rules linked to confirmed vulnerabilities) and not file scanning, it's faster, more accurate, and protects your site proactively.

THE HIDDEN COST OF SCANNING

This should not be overlooked: scanning repeatedly every file for malware means the plugin reads everything on your site. This puts heavy load on CPU, memory, and disk — especially on shared hosting — for a very low added value, unless you know that your website has been corrupted.

The ideal WordPress security solution

The ideal WordPress security solution should solve the challenges agencies face by protecting sites across five key security fronts:

5 SECURITY FRONTS	TOOLS TO USE
Shows you what's exposed	Vulnerability monitoring and website health checks
Shut the doors hackers use	Security hardening and automatic updates
Stops attacks in real time	Firewall and Virtual Patching
Catches what slips through	Transparent activity log and malware scanner
Helps you recover fast	Reliable backups and cleanup measures

The current reality is that not a lot of WordPress security solutions cover all this. Many of them focus on just one part of the security lifecycle. Some specialize in prevention with firewalls and hardening. Others focus on detection through monitoring and activity logs. Others are built mainly for recovery with malware scanning and cleanup.

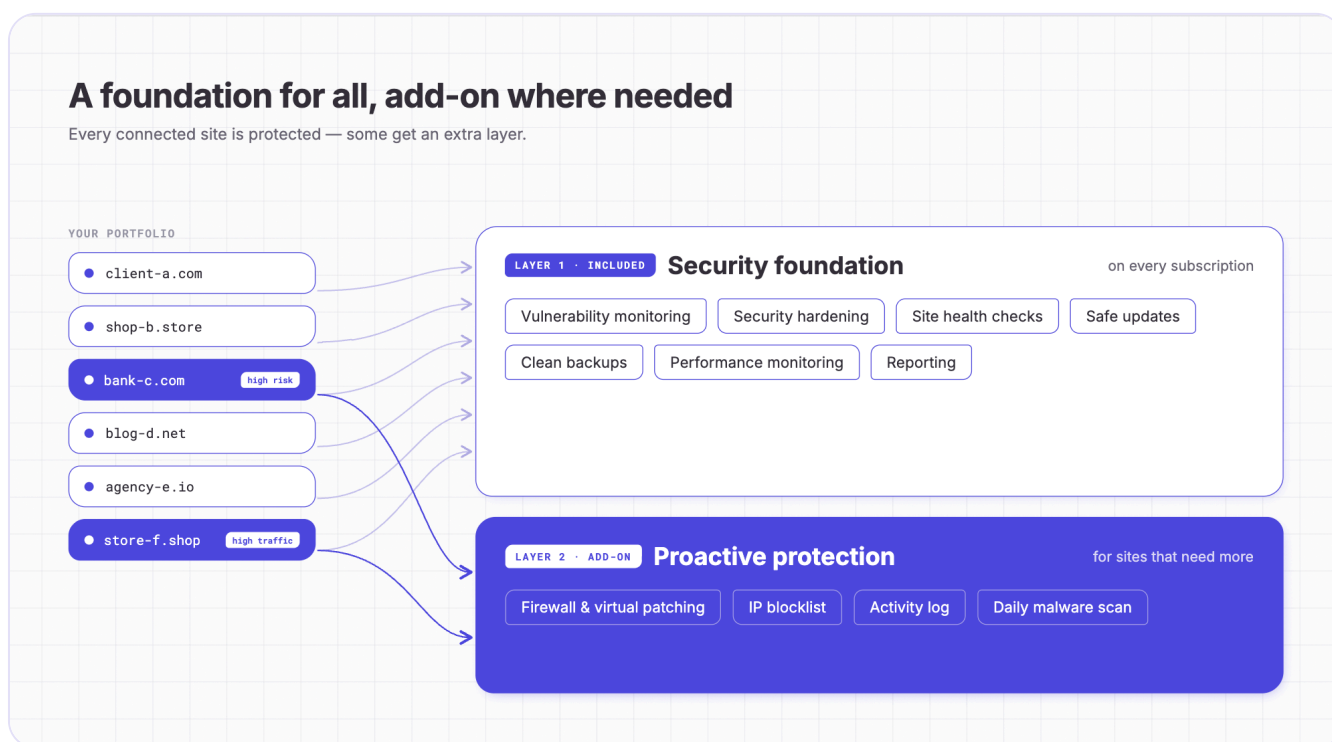
As a result, WordPress professionals often need several tools to cover the full security lifecycle. This adds cost, complexity, and more plugins that can affect site performance. WP Umbrella addresses this gap. Here's how.

How does WP Umbrella secure your full portfolio?

First of all, as an all-in-one WordPress management platform, WP Umbrella brings security into the same workflow you already use to manage your WordPress maintenance tasks. This is important because security should not be performed in a bubble.

Backups, updates, uptime, performance, and security are all part of WordPress maintenance. They should work together, so you can spot a problem and take action quickly and as part of the same workflow.

Having the best vulnerability monitoring means little if you don't run the update that fixes the problem. And the best malware scanner is not enough if you don't have a clean backup to restore. Put simply, security works best when it's part of the bigger WordPress maintenance workflow — and WP Umbrella allows exactly that. Then it splits it into two main layers.



LAYER 1 · SECURITY BASE

Vulnerability monitoring and alerting, WordPress hardening, safe automatic updates, and site health checks.

LAYER 2 · SECURITY ADD-ON

Proactive protection through the firewall and virtual patching, a shared blocklist of malicious IPs, a security-driven activity log and a malware scanner.

Four core capabilities, on every site

In the first layer WP Umbrella includes four core security capabilities. These are considered a must-have, so they're included with every subscription, with no add-on required.

01 WordPress vulnerabilities monitoring across your full portfolio

WP Umbrella checks every site in your portfolio every six hours for known vulnerabilities affecting WordPress core, plugins, and themes. You can also run a manual scan whenever you want instead of waiting for the next automatic check.

These checks are powered by Patchstack. When a vulnerability is found, you can see which plugin or theme is affected, how serious the problem is, and which version fixes it.

Every site's security, on one screen

Protection score, vulnerabilities, health and attacks blocked — across the whole portfolio.

Security dashboard

Global protection score **56/100**

5 Sites with concerns

Vulnerabilities [Fix vulnerabilities](#)

2 Critical 4 Medium or Low

PHP versions

3 No secured 4 Not supported

Site Protect add-on [Deploy](#)

5 Site unprotected

Sites	Protection score	Vulnerabilities	Site health	PHP Version	Security add-on
 WP Engine wpumbrella1.wpenginepowered.com	99/100	0 vulnerability	1 warning	8.4.23	 2 attacks blocked
 Rocketnet EU fwusi7bx1g.onrocket.site	84/100	0 vulnerability	2 warnings	7.4.33	
 Rocket.net US o2m3a1rx01.onrocket.site	84/100	0 vulnerability	2 warnings	7.4.33	
 WP Umbrella wp-umbrella.com	15/100	13 vulnerabilities	1 warning	8.1.32	 1 attack blocked
 Airwax airwaxfreely.com	8/100	60 vulnerabilities	3 warnings	7.4.33	

02 Automatic security updates, independent from your regular schedule

Once the security fix becomes available, you can apply the update straight from the dashboard, with one click, across every affected website. But you can also take this one step further and automate WordPress security updates entirely.

With this option enabled, security fixes are installed as soon as they become available, without waiting for your regular WordPress update schedule. This helps you stay one step ahead of new threats while reducing the work needed to keep your portfolio secure.

03 WordPress security hardening rules from one place

You can apply WordPress hardening settings with simple toggle buttons, site by site or all at once. This gives you control over the security baseline for each website without having to configure everything from scratch.

Every hardening protection, in one panel

Flip each protection on individually — or enable them all in a single click.

Protections

Turn hardening protections on for this site.

[Enable all](#)[Disable all](#)

Hide your WordPress version

Removes the WP version from your HTML and feeds so attackers can't target version-specific exploits.



Block user enumeration

Stops bots listing your usernames through author pages and the REST API before a brute-force attack.



Mask login error messages

Shows a single generic message on failed logins so attackers can't tell whether a username exists.



Disable the theme and plugin file editor

Removes the built-in code editor from wp-admin so a compromised account can't inject PHP.



Add security headers

Sends hardening HTTP headers such as X-Frame-Options to protect against clickjacking and content sniffing.



Rate-limit login attempts

Throttles repeated failed logins from the same source to slow down brute-force attacks.



Block known malicious IPs at login Requires Security add-on

A self-learning module shares a blocklist across every site, stopping flagged IPs before they reach yours.



Disable XML-RPC

Closes the XML-RPC endpoint attackers abuse to amplify brute-force attempts and pingback DDOS.



Protect your uploads folder

Blocks PHP files from running inside your uploads folder, with an automatic rollback if your site is affected.



04 Site health checks as your WP Umbrella security assistant

WP Umbrella's Site Health Assistant checks for common issues across your websites, including:

SSL configuration

WordPress and PHP versions

Search engine visibility

WP_DEBUG

Inactive plugins and themes

Results are split into Attention Needed and Passed, so your dashboard stays focused on the things that need your attention and nothing slips through, no matter how minor.

What needs attention, what's already passing

Every routine health check on one screen — issues surfaced first, with a fix on hand.

Attention needed 2

[Expand all](#)

php

We recommend a PHP update

Dismiss ^

PHP versions that no longer receive patches expose your site to known vulnerabilities.

Your current PHP version (**7.4.33**) is outdated and no longer supported. [Outdated PHP versions](#), such as those prior to 8.3, are considered end-of-life and are no longer patched.

🔌

9 plugins are inactive

Deactivated plugins still expose code that attackers can probe.

[Delete deactivated plugins](#)

Dismiss v

Passed 5

✓

Your site uses the SSL protocol.

HTTPS is properly configured for this site.

✓

Your WordPress version is up to date (7.0.2).

Running WordPress 7.0.2.

✓

Your site is indexable by search engines.

Search engines can crawl and index your content normally.

✓

Your WP_DEBUG is set to false.

WP_DEBUG is off in production. No sensitive output exposed.

✓

You don't have any inactive themes.

Only the active theme remains. No unused theme code on disk.

Four extra tools around every site that needs more

The security foundation gives every site a strong starting point. But some clients require more active protection. The Security add-on adds four extra tools that help you block attacks, stop known threats, spot suspicious activity, and find malware. Basically, it brings the key security measures available in the WordPress ecosystem into one lightweight solution.

The WP Umbrella Security add-on

Four active layers around every site that needs more.



Firewall & virtual patching

Blocks exploits at the PHP level while you wait for the fix.



Shared IP blocklist

An attacker flagged on any site is blocked on all of them.



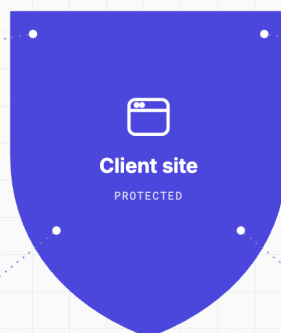
Activity log

Watches 8 kinds of suspicious activity — who, what, when.



Daily malware scan

Checks every day; cleanup on demand for real infections.



01 Firewall and Virtual Patching that stop attacks before they happen

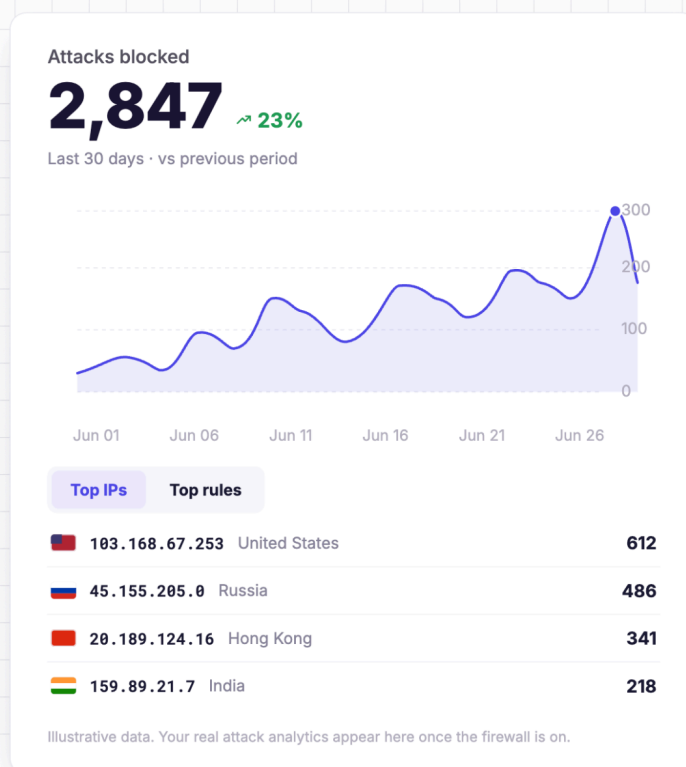
As explained in section 0.0 from this guide, sometimes a security vulnerability is found by hackers before the developer has released a fix. WP Umbrella integrates the virtual patching technology, powered by Patchstack, to help protect your site during this gap.

You can also see what the firewall has blocked. The Insights view shows attacks blocked in the last 30 days, the IP addresses behind them, and the rules that stopped them. This gives you a clear view of the protection running on your sites and useful information to share with clients.

The firewall is designed to have no negative impact on site performance and works alongside network and server-level firewalls provided by your hosting infrastructure.

Every blocked attack, counted and traced

Virtual patching shields a flaw until the official fix is safe to apply.



02 Block known attackers before they reach your site

Hackers often attack more than one website. If an IP address is trying to break into one site, it may try to attack another.

WP Umbrella watches login attacks across every site on the platform and continuously builds a shared blocklist of malicious IP addresses. Once an IP is flagged anywhere on the network, it's blocked on your site before it gets a chance to attack it, protecting every other site from the same threat.

03 Know when something suspicious happens

Stopping attacks is only part of security. You also need to know when something unusual happens on a website. The built-in Activity Log checks for eight types of suspicious activity, including:

Brute-force login attempts

New admin accounts

Sign-ins from new locations

File changes

Critical settings changes

Mass content deletion

Hidden administrator accounts

.htaccess changes

When something needs your attention, you can see what happened, who was involved, the IP address, and when it happened.

You also get the information you need to understand the problem and decide what to do next. You can search the full activity log at any time to see what has happened across your sites.

One log watching for suspicious activity

It flags the one thing that needs a look and keeps everything else quietly recorded.

Activity Log

Enabled

Needs attention 1

**Sign-in from a new location**

wphealth signed in from a location we've never seen for this account. Confirm it was them — if not, reset the password and turn on 2FA.
Last occurrence: Jul 14, 2026 05:41

[View details](#) [Dismiss](#)

All clear 7

 Brute-force attempts

 New admin access

 File integrity monitoring

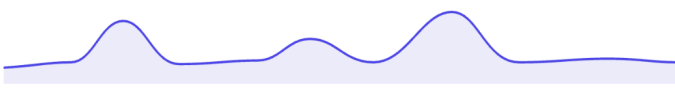
 Critical settings changed

 Mass content deletion

 Hidden administrator accounts

 .htaccess protection changed

Events recorded
930
Jun 22 – Jul 22



04 Scan for malware every day, with zero load on your sites

Even with good protection, some attacks may still get through. That's why WP Umbrella's Malware Scanner checks your sites for malware every day, entirely from its own infrastructure. Nothing runs on your server, so scanning adds zero load to your sites.

The scan goes deep: WordPress core, free and paid plugin and theme files (including ones that never came from the official store), your wp-content and uploads folders, scheduled tasks, and supply chain changes. It catches more than known threats — it's built to find hidden malware and code no vulnerability database has seen yet.

Anything it flags appears in your dashboard with the date it was found. If you check a file and know it's safe, you can dismiss it so it doesn't keep showing up as a threat. If the scanner finds a real infection and you need to recover your site, clean backups are ready to restore with just one click straight from the WP Umbrella dashboard.

BEFORE, DURING, AFTER

Together, these four capabilities help protect your sites before, during, and after an attack. The firewall and blocklist help stop threats. The activity log helps you spot problems early. And the malware scanner helps you find and clean up infections that get through.

WP Umbrella vs. traditional WordPress security plugins

Here's how WP Umbrella holds up against running a traditional security plugin on every site:

	TRADITIONAL SECURITY PLUGINS	WP UMBRELLA
Security lifecycle	Usually covers one stage: prevention, detection, or recovery	Covers security end-to-end: prevention, detection, and recovery together
Portfolio view	A separate dashboard per site, or a separate paid console	One dashboard, every site. Tied in with backups, updates, uptime and performance monitoring.
Performance	Scanning and firewall logic run inside WordPress, on every site, adding to CPU and memory load	Scans run entirely off your servers, zero load. Firewall runs at the PHP level, no measurable impact
Client reporting	Manual, site by site	Built into your automated maintenance reports
Pricing	Per site, or in bundles that don't scale and adapt as your portfolio changes	2€ per site, per month. +2€ security add-on on the sites that need it.

WP Umbrella easily replaces Wordfence, Sucuri, Solid Security, and similar WordPress security plugins. What it doesn't replace is your hosting provider's network-level firewall or a CDN like Cloudflare — those stay part of your infrastructure, and WP Umbrella's firewall works alongside them rather than instead of them.

FROM THE FIELD



The Security Add-on is incorporated in WP Umbrella, with the goal of delivering the highest level of WordPress security for all users. The security stack agencies used to bolt together (virtual patching, malware scanner, activity log, hardening) is now one system inside the platform their care plans already run on.

Aurelio Volle • CEO at WP Umbrella

WordPress security and maintenance in one place

As we reach the end of this guide, we hope one thing is clear: WordPress security doesn't work in isolation. Keeping sites secure isn't just about blocking attacks. It's also about keeping software up to date, having clean backups ready, monitoring your sites, and knowing what's happening across your portfolio.

That's why WP Umbrella brings security together with backups, updates, uptime, performance monitoring, and client reporting in one platform. Instead of stitching together separate tools, you manage everything from one place and keep your security standards consistent as your portfolio grows.

On top of security, WP Umbrella also allows you to

- 01 See all your sites at a glance and spot where attention is needed fast.
- 02 Schedule GDPR-compliant, encrypted backups (hourly, daily, or weekly) with one-click restores.
- 03 Automatically update WordPress core, plugins, and themes in bulk.
- 04 Monitor uptime and performance (PageSpeed, Core Web Vitals, load times, etc.).
- 05 Get real-time alerts via email or Slack when something goes wrong.
- 06 Send automated, professional maintenance reports to clients, fully branded and personalized.

3.0 Learning to fly

- 1 Proactive WordPress security can be ensured with virtual patching. Virtual patching is a security method that blocks known exploits before they reach vulnerable code, without modifying or weighing down the website itself.
- 2 Traditional security scanners detect infections after they happen, and can slow down your site. Virtual patching blocks known exploits before they reach your site, making protection faster, lighter, and proactive.
- 3 The ideal WordPress security solution should cover five fronts: exposure, prevention, real-time blocking, detection, and recovery. Most tools only cover one or two.
- 4 WP Umbrella covers all five security fronts across two layers. Layer 1 (free with every subscription): vulnerability monitoring, automatic security updates, hardening, site health checks. Layer 2 (Security add-on): Firewall & Virtual Patching, a shared IP blocklist, an Activity Log, and a daily malware scanner that runs off your servers.
- 5 Unlike traditional security plugins, WP Umbrella brings security together with backups, updates, uptime monitoring, performance monitoring, and client reporting in one centralized platform, with no measurable performance cost.
- 6 Patchstack is the leader in open-source vulnerability intelligence, covering the entire lifecycle from detection to mitigation. Their virtual patching technology powers one of the most essential parts of WP Umbrella's Security Add-on.

READY TO TRANSFORM YOUR WORDPRESS MANAGEMENT?

Stay ahead of security threats and save hours on maintenance work.

Bring WordPress security, backups, updates, performance monitoring, client reporting, and more into one platform built for agencies.

Start your free trial →

app.wp-umbrella.com/register

4,9

G2 REVIEWS

4,7

TRUSTPILOT

4,8

WP REPOSITORY

THIS GUIDE IS DEVELOPED WITH

 **patchstack**